Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 14, 2021

N. Cook
V. Bertola
Open-Xchange
A. Fidler
BT plc
N. Leymann
Deutsche Telekom
R. Weber
Akamai

July 13, 2020

A Proposal for a DoH Discovery Trial
draft-cook-doh-discovery-trial-00

Abstract

The following document describes a proposal for a trial of an experimental mechanism for the discovery of DNS-over-HTTPS resolvers provided by Internet Service Providers to their customers.

Status of This Memo

Copyright Notice

1. Introduction

The introduction of encrypted DNS transport protocols like DoH (DNS-over-HTTPS [RFC8484]) can provide additional confidentiality to Internet users that need a DNS resolution service to access online resources. Most end-users currently get their DNS resolution service from the Internet Service Provider that also supplies them with Internet access; thus, to promote a straightforward migration path from unencrypted to encrypted DNS transport and to avoid the issues deriving from a change of DNS provider, it would be useful to establish a mechanism through which stub DNS resolvers on the user's device can discover under appropriate security conditions whether the local network provides a DoH resolver, and if so, start using it automatically. This DoH deployment model will be referred to as "same provider auto-upgrade".

This document describes an experimental mechanism which was developed by a group of Internet Service Providers and DNS implementers for that use case, based on the use of a DNS query for a special use domain name. It is intended as an informational document to support and encourage other parties to join the experiment.

2. Requirements Notation and Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Throughout this document, values are quoted to indicate that they are to be taken literally. When using these values in protocol messages, the quotes MUST NOT be used as part of the value.

3. Rationale

The IETF ADD Working Group was approved by the IESG in February 2020; an extract from the charter [ADD] follows:

"This working group will focus on discovery and selection of DNS resolvers by DNS clients in a variety of networking environments, including public networks, private networks, and VPNs, supporting both encrypted and unencrypted resolvers. It is chartered solely to develop technical mechanisms. Making any recommendations about specific policies for clients or servers is out of scope."

To support the achievement of this technical objective, non-technical considerations also come into play. There is a desire to maximise the number of users that can enjoy an easy upgrade path towards DNS encryption, by making it possible for customers of ISPs that deploy DoH interfaces to their resolvers to get upgraded automatically.

The early discovery mechanisms implemented by some browsers cannot cope with home networks advertising the CPE's private IP address as the endpoint for the local DNS resolver, and thus would exclude the fixed broadband and home mobile router customers of a significant number of ISPs (including the major ones in Europe) from access to this new technology, depending on their Internet access network architecture and on their ease of upgrade of CPEs.

Additionally, in Europe regulation requires all ISPs to allow users to connect to the Internet with any home router of their choice, so it is not even possible for ISPs to prevent the use of home routers that do not support any other DNS resolver mode than dnsmasq over a private IP address.

Regardless of the outcome of IETF and policy discussions, it is likely that any fully fledged, standard discovery protocol will take a relatively long time to reach consensus. Therefore this document proposes an interim solution, which combines in-band discovery with out-of-band protections such as those already used by Google Chrome and Microsoft Windows (i.e. pre-vetting of DoH services, plus some additional protections as discussed below).

This solution would allow participating ISPs using DNS forwarders in their CPEs to provide DoH resolver services to their users in a short timeframe, as long as they used clients (browsers and operating systems) that participate in this trial.

The proposed solution is described in the following section.

4. The Proposed DoH Discovery Trial

4.1. How ISPs Join the Trial

Out-of-band (e.g. through the already established process, or through direct contact at industry venues such as EDDI [EDDI]), ISPs make it known that they would like client vendors to discover their DoH service, but have a significant proportion of users who are using CPEs which act as forwarders.

Each participating vendor, depending on their own security policies, decides if they are fine with an open DNS-based discovery of the local resolver, or if they want to reduce the potential attack

surface by restricting the resolvers that the local network can advertise. Section 5.2. describes the security implications of such a choice.

In the latter case, participating ISPs, regardless of whether they plan to offer public DoH services, guarantee that they (also) offer a DoH service on a URI which is closed, i.e. only accessible from their own network and not from the Internet, and whose hostname is located within a domain name owned by the ISP; this is the DoH service that can be enrolled in the program for vendors that require such restriction. We will refer to these DoH services as "closed resolvers".

This restriction prevents malicious actors from switching a user's DNS resolution to an off-net DNS resolver which is also a trial participant. (However it does not prevent switching from an off-net to an on-net resolver; see section 5). It is up to each DoH client vendor whether they choose to validate (once or continuously) such a guarantee.

The ISPs then provide the vendors with the URI(s) of their (optionally closed) DoH service(s). The URI must contain an FQDN; IP addresses are not acceptable. These URIs are added to a list maintained by the DoH client vendor. For the purposes of this document, we shall call this list the "whitelist" of DoH servers corresponding to ISP resolvers reached via CPEs; it could be a different list from the list of public DoH services used by the current auto-upgrade mechanisms.

4.2. Proposed DoH Resolver Discovery Logic

This process only starts if the configured Do53 resolver is a private ([RFC 1918]) IPv4 or IPv6 link local or unique local address. The auto-upgrade of resolvers with public IP addresses is outside of the scope of this document, though participating vendors, if they want, can use this mechanism for that purpose as well.

The client performs over Do53 (traditional DNS) a TXT record lookup for dohresolver.arpa, a specifically chosen special use domain name (SUDN) [RFC6761]. Eventually, if this mechanism gains adoption, it may be appropriate to register this name with IANA, but we do not anticipate any problems using it on an interim basis, since it is restricted to specific resolvers and does not affect the wider DNS or the arpa TLD. Also, it would be easy to move to any other SUDN that might be standardized by the IETF.

The resolver is configured to respond to that SUDN with a TXT record containing the URI template of the DoH service.

If the Do53 response is anything other than a TXT answer, the discovery is terminated. As a note, some browser makers reported that they sometimes have difficulties with performing lookups on DNS records other than A/AAAA. If CPE routinely filter/drop TXT record lookups, then this approach will not work. To our knowledge, none of the CPE of the ISPs providing data for this document do any modification or filtering of TXT records, and common forwarding software such as dnsmasq does not appear to have issues with arbitrary RRs. Any more facts on this topic would be useful.

In the event of no response being received, the client should decide its own retry policy for the dohresolver.arpa query, but we recommend one or more retries are performed to mitigate packet loss or temporary high load.

In the event of a successful response, the client - if so desires - can check whether the URI in the response matches one of the (optionally closed) DoH URIs that have been added to the "whitelist", and discard it if not.

In the event of a successful response which points to an acceptable DoH resolver, it is up to the DoH client vendor what happens next, for example:

- Auto-upgrade takes place - i.e. connection is attempted to that URI. Assuming that certificate validation and TLS handshake succeeds etc., resolution switches to the DoH service, otherwise the client continues to use the Do53 service.

- The user is presented with a dialog asking them if they'd like to use the newly discovered DoH server. If they accept, then connection proceeds as above.

- The DoH server is added to a list of manually selectable DoH servers.

- Any other suitable logic, e.g. ignoring the response for policy reasons.

The DoH client should respect the TTL of the TXT record returned, and perform a new DNS lookup upon expiry.

4.3. Effect on Possible Use Cases

The basic policy principle for the existing auto-upgrade methods is to avoid changing the resolver that the user has chosen either explicitly (i.e. through manual configuration) or implicitly (e.g. via DHCP).

This logic attempts to preserve that as far as practically possible, through use of the TXT record lookup; the lookup will only return a valid answer if the resolver being used has actively created an authoritative TXT record for the dohresolver.arpa domain. This assumes no malicious actors; see section 5 for security considerations.

We will now discuss the impact of running such an experiment in real world use cases, showing the behaviour that will occur for customers of participating ISPs using participating clients if the DoH client follows the logic described in this proposal. The four possible scenarios for a consumer setup cover all the possible variations of resolver/forwarder configuration and downstream resolver. If either the ISP or the client does not participate in the experiment, no auto-upgrade will ever happen.

This is the effect of the proposed logic in the different scenarios:

1. The user is using an ISP-supplied CPE, which forwards Do53 traffic to the ISP's Do53 resolver. The ISP's Do53 resolver will return a TXT record for dohresolver.arpa, and thus auto-upgrade will take place. The client will then bypass the forwarder, directing queries via DoH directly to the ISP's resolver.

2. The user manually configured a local DNS forwarder themselves (e.g. an off-the-shelf CPE, or they run dnsmasq on a local server) to forward queries to their local ISP resolver. This resolver will return a TXT record for dohresolver.arpa, and thus auto-upgrade will take place, bypassing the forwarder, exactly like in the previous case.

3. The user has manually configured a local DNS forwarder themselves (e.g. an off-the-shelf CPE, or they have modified the ISP-provided CPE) to forward to a resolver that is not the ISP resolver, e.g. 1.1.1.1 or 9.9.9.9. These resolvers will return NXDOMAIN for dohresolver.arpa, and thus no auto-upgrade will take place.

4. The user has manually configured a local DNS resolver themselves (e.g. Raspberry PI or similar). This resolver will return NXDOMAIN for dohresolver.arpa, and thus no auto-upgrade will take place.

From the DoH client's perspective, all four scenarios are the same (i.e. the system resolver has a RFC1918 IPv4 or IPv6 link local or unique local address), and whether that resolver was configured via DHCP or manually would not appear to matter that much. Scenarios 3

and 4 can be discounted because no action takes place, however scenarios 1 and 2 do have the effect of bypassing the forwarder.

There is a semantic difference between scenarios 1 and 2; in scenario 2 the user may have configured a forwarder deliberately, for example to do filtering, caching, logging or innumerable other reasons. For that reason, DoH client vendors need to consider whether the above scenarios, (or any additional scenarios not considered above), justify asking for the user's consent to the upgrade to DoH directly to the ISP resolver (and thus bypassing any intermediate forwarders).

Moreover, in cases 3 and 4 it would be easy for the operator of the alternative resolver (whether it is another DNS operator, as in case 3, or the user themselves, as in case 4) to also allow auto-upgrade to DoH of the connection, simply by configuring their own resolver to reply to the query for dohresolver.arpa. However, if the client vendor chooses to restrict the auto-upgrade mechanism only to whitelisted URIs, then these other operators would need to also join the experiment; in case 3, this could be made impossible by the restriction itself, as by definition the resolver in this case is an "open" one, and the vendor would need to partially lift the restriction and accept known open DoH resolvers from a separate whitelist; in case 4, this could be made impossible by the non-technical requirements of the procedure for joining.

5. Security Considerations

5.1. Existing Auto-Upgrade Mechanisms

The security objective for current same-provider auto-upgrade mechanisms is to ensure that the client is talking to the same resolver operator as before, but now over DoH. On-path attackers have no way to influence this, since the mechanism is based on the client knowing the public IP address of the existing resolver and a pre-configured URI template for the auto-upgrade DoH resolver for that IP address.

5.2. Current Proposal

This proposal does not use the same threat model as the existing auto-upgrade solution. The differences are discussed below.

On-path attackers could perform a downgrade attack. However, given that current auto-upgrade mechanisms do not work for users with forwarders in their CPE, such a downgrade attack would result in the same situation as currently, i.e. the client would continue to use Do53. However, given this threat, the upgrade to DoH can only be considered as opportunistic security.

On-path attackers could change the discovery response from that returned by the actual configured resolver. There are two scenarios that need to be considered, depending on the vendor's policy.

If the DoH client vendor enforces the "closed resolver" restriction, then the following applies:

- Given that the client will only accept auto-upgrade via discovery to a "closed resolver", there is only one resolver that will be accepted by the client via the discovery mechanism - the DoH resolver offered by the user's ISP. (This assumes that the ISP is diligent about ensuring their resolver is actually closed - this could be verified periodically by the vendors).

- There exists a risk that an on-path attacker could redirect a user from a manually selected resolver (configured manually by the user on the CPE/forwarder) to the resolver provided by the local ISP. This would have the effect of moving the user from a resolver that they did select (e.g. 9.9.9.9) to one they did not select. Such a risk is not mitigated by this proposal. Note that this risk exists only when there is an on-path attacker, since the discovery query happens via DNS and thus goes to the resolver originally chosen by the user.

If the DoH client vendor does not enforce the "closed resolver" restriction, then the following applies. An on-path attacker could redirect a user from a manually selected resolver (configured manually by the user on the CPE/forwarder) to any resolver on the "whitelist" of DoH servers. This would have the effect of moving the user from a resolver that they did select to one they did not select. Such a risk is not mitigated by this proposal. Note that this risk exists only when there is an on-path attacker, since the discovery query happens via DNS and thus goes to the resolver originally chosen by the user.

In both of the above use cases, the only possible end result of a successful attack aimed at changing resolvers is that a user has moved from an insecure Do53 service whose results are controlled by a malicious on-path attacker, to a secure DoH service which is on the DoH client's "whitelist". The on-path attacker has only succeeded in moving the user to a vendor-verified resolver over which they have no control, and which they cannot use for further attacks; as long as the vendor's whitelisting process is secure, an attacker wishing to gain control of the user's DNS resolution process for further steps, e.g. to redirect the user's Web requests to a phishing page, would not be able to do so through this attack. This would apply even if the new DoH resolver were open, as long as it is on (the same or another) vendor-verified whitelist. However, the user has still

moved to a resolver operated by a different organization which is almost certainly not what the user "wanted"; hence the possible need for user confirmation.

The security assumptions regarding the "closed resolvers" above are predicated on the participating ISPs performing the appropriate actions to "close" their resolver(s) to the public internet, thus making them only available to customers on their network. DoH client vendors relying on the security assumptions provided by this may wish to make periodic checks (see section 6) to ensure that listed DoH resolvers are indeed not accessible from the public internet, otherwise new attacks would be possible such as an on-path attacker redirecting a user from their currently selected resolver to the resolver of another participating ISP.

In the end, vendors that adopt the approach of vetting and whitelisting DoH resolvers before allowing users to auto-upgrade to them will always enjoy a certain degree of reassurance on the legitimacy of those resolvers (though at the expense of excluding the users of other DoH resolvers, including self-managed resolvers that people may install on their home networks, from automatic upgrade).

Without the additional "closed resolver" restriction, an attacker may succeed in redirecting the user to any of the whitelisted DoH services, while with that additional restriction, an attacker may only succeed in redirecting the user to the ISP's own closed DoH service, if the user is not already using it. Whether this gain in security is worth the additional organizational complexity is for each vendor to consider; we expect that running this experiment could also allow to evaluate how useful that additional restriction could be in practice.

6. Implications for Vendors

The experiment requires participating vendors to change their current implementation of the auto-upgrade mechanism and add the logic described.

For DoH client vendors enforcing the "closed resolver" restriction, some additional vetting and active checking of "auto-upgrade" DoH providers would be necessary, to ensure that ISP resolvers are indeed "closed" and only accessible to customers on their own networks, as assumed in Section 5 above. This could take the form of periodic attempts to connect to all the DoH URIs on the "whitelist" from a variety of locations known to be outside of any service provider networks. It would be up to the organisation responsible for the DoH client to decide how stringent this check should be. For example, it

may involve automated weekly checks, and alerts to ISPs whose resolvers do not meet the required standards.

DoH client vendors who also support the "auto-upgrade based on public resolver IP" logic need to maintain two "whitelists"; DoH servers could of course be on both lists, or both lists could be merged into one with additional parameters for each featured resolver, as preferred.

7. Acknowledgements

This document is the product of an informal group of experts including the following people:

Alister Winfield, Sky

Andrew Campling, 419 Consulting

Andy Fidler, BT plc

Chris Box, BT plc

Gianpaolo Scalone, Vodafone

Neil Cook, Open-Xchange

Nic Leymann, Deutsche Telekom

Norman Kowalewski, Deutsche Telekom

Ralf Weber, Akamai

Vittorio Bertola, Open-Xchange

The authors would like to thank Kenji Baheux and Eric Orth (Google) and Tommy Jensen (Microsoft) for their feedback and suggestions.

8. References

8.1. Normative References

[ADD] IETF, "Adaptive DNS Discovery (ADD) Working Group", February 2020, <https://datatracker.ietf.org/wg/add/about/>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", RFC 6761, DOI 10.17487/RFC6761, February 2013, <https://www.rfc-editor.org/info/rfc6761>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

8.2. Informative References

[EDDI] EDDI, "Encrypted DNS Deployment Initiative", July 2020, <https://www.encrypted-dns.org/>.

Authors' Addresses

Neil Cook
Open-Xchange Ltd
7 Gerard Street
Ashton-in-Makerfield, Wigan, Greater Manchester WN4 9AG
United Kingdom

Email: neil.cook@noware.co.uk
URI: https://www.open-xchange.com/

Vittorio Bertola
Open-Xchange Srl
Via Treviso 12
Torino 10144
Italy

Email: vittorio.bertola@open-xchange.com
URI: https://www.open-xchange.com/

Andy Fidler
BT plc
BT Adastral Park
Martlesham Heath, Ipswich IP5 3RE
United Kingdom

Email: andrew.fidler@bt.com
URI: https://www.bt.com/

Nicolai Leymann
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
Bonn 53113
Germany

Email: N.Leymann@telekom.de
URI: https://www.telekom.com/

Ralf Weber
Akamai Technologies GmbH
Parkring 20-22
Garching 85748
Germany

Email: ralf.weber@akamai.com
URI: https://www.akamai.com/